



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/904,010

07/11/2001

Bruce K. Martin JR.

3399P042

1786

26529

7590

12/01/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN/PDC  
12400 WILSHIRE BOULEVARD  
SEVENTH FLOOR  
LOS ANGELES, CA 90025

EXAMINER

ABRISHAMKAR, KAVEH

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 12/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/904,010

Applicant(s)

MARTIN ET AL.

Examiner

Kaveh Abrishamkar

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 06 September 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 15-26,32-38 and 40-55 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 15-26,32-38 and 40-55 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>06/05/06, 09/06/06</u> . | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on September 6, 2006 has been entered.

2. Claims 15-26, 32-38, and 40-55 are currently being considered.

### ***Response to Arguments***

3. Applicant's arguments, see Applicant's remarks pages 12-21, filed September 6, 2006 with respect to the rejection(s) of claim(s) 15-26, 32-38, and 40-55 under Soursa (U.S. Patent Pub. No. US 2002/0194584 A1) and Ramasubramani (U.S. Patent No. 6,233,577) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Penders (U.S. Patent No. 6,880,080).

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 15-26, 32-38, and 40-55 are rejected under 35 U.S.C. 102(e) as being anticipated by Penders (U.S. Patent 6,880,080).

Regarding claim 15, Penders discloses:

A method comprising:

operating a primary trusted provisioning domain (TPD) (column 5 lines 1-13), wherein the primary TPD is interpreted as being the Certificate Authority (CA); and using the primary TPD to provision a mobile device on a wireless network by sending a provisioning message to the mobile device, the provisioning message specifying a secondary TPD authorized to provision the mobile device via a network and an identifier of one or more parameters which the secondary TPD is authorized to provision, the secondary TPD comprising a provisioning server (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain functions.

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Penders discloses:

A method as recited in claim 15, wherein the primary TPD is within a trusted environment, and wherein the secondary TPD is outside the trusted environment (Figure 1, column 5 lines 1-14), wherein the certificate authority is connected via a telecommunications network to the terminal and the Service Provider.

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Penders discloses:

A method as recited in claim 16, wherein the secondary TPD communicates with the mobile device via a second network that is outside the trusted environment (Figure 1, column 5 lines 1-14), wherein the certificate authority is connected via a telecommunications network to the terminal and the Service Provider.

Claim 18 is rejected as applied above in rejecting claim 16. Furthermore, Penders discloses:

A method as recited in claim 16, further comprising using the primary TPD system to provision the mobile device with a digital certificate identifying the secondary TPD to enable the secondary TPD to provision the mobile device using a digital signature (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Claim 19 is rejected as applied above in rejecting claim 15. Furthermore, Penders discloses:

A method as recited in claim 15, wherein the provisioning message specifies a plurality of secondary TPDs authorized to provision the mobile devices and one or more parameters which each of the secondary TPDs is authorized to provision (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device, and wherein there can be more than one service provider (column 5 lines 5-13).

Regarding claim 20, Penders discloses:

A method comprising:

operating a primary provisioning server within a predefined trusted environment, the primary provisioning server having authorization to provision a plurality of mobile devices on a wireless network (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain functions;

using the primary provisioning server to provision a digital certificate of the primary provisioning server in each of the mobile devices (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate

specifying that the Service Provider (secondary provisioning server) is allowed to perform certain function;

using the primary provisioning server to provision a digital certificate of a secondary provisioning server in the mobile devices, wherein the secondary provisioning server is on a second network outside the trusted environment (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain functions; and

using the primary provisioning server to provision the mobile devices with information indicating to the mobile devices authorization of the secondary provisioning server to provision the mobile devices (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Claim 21 is rejected as applied above in rejecting claim 20. Furthermore, Penders discloses:

A method as recited in claim 20, wherein the primary and secondary provisioning servers each use their respective digital certificates when provisioning the mobile devices, to enable the mobile devices to authenticate provisioning messages from the primary and secondary provisioning servers (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Claim 22 is rejected as applied above in rejecting claim 20. Furthermore, Penders discloses:

A method as recited in claim 20, further comprising using the primary provisioning server to specify one or more parameters which the secondary provisioning server is authorized to provision in the mobile devices (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Claim 23 is rejected as applied above in rejecting claim 20. Furthermore, Penders discloses:

A method as recited in claim 20, further comprising using the primary provisioning server to provision the mobile devices with information indicating authorization of a plurality of secondary provisioning servers to provision the mobile devices (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device, and wherein there can be more than one service provider (column 5 lines 5-13).

Claim 24 is rejected as applied above in rejecting claim 23. Furthermore, Penders discloses:



A method as recited in claim 23, further comprising using the primary provisioning server to specify one or more parameters which each of the secondary provisioning servers is authorized to provision in the mobile devices (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Penders discloses:

A method as recited in claim 24, wherein said using the primary provisioning server to specify one or more parameters comprises assigning each of the secondary provisioning servers provisioning authorization of a different scope (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device, wherein the functions can be different between different service providers (column 5 lines 44-61).

Claim 26 is rejected as applied above in rejecting claim 20. Furthermore, Penders discloses:

A method as recited in claim 20, wherein the primary provisioning server has unrestricted authorization to provision the mobile devices, and authorization of the secondary provisioning server to provision the mobile devices is regulated by the

primary provisioning server (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device, wherein the functions can be different between different service providers (column 5 lines 44-61).

Regarding claim 32, Penders discloses:

A machine-readable program storage medium storing instructions which, when executed in a processing system, configure the processing system to operate as a primary provisioning server within a predefined trusted environment, the primary provisioning server having authorization to provision a plurality of mobile devices on a wireless network, such that the instructions configure the processing system to execute a process comprising:

provisioning a digital certificate of the primary provisioning server in each of the mobile devices (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain function;

provisioning a digital certificate of a secondary provisioning server in the mobile devices, wherein the secondary provisioning server operates outside the trusted environment (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain functions; and

provisioning the mobile devices with information indicating to the mobile devices authorization of the secondary provisioning server to provision the mobile devices (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Claim 33 is rejected as applied above in rejecting claim 32. Furthermore, Penders discloses:

A machine-readable program storage medium as recited in claim 32, wherein the primary and secondary provisioning servers each use their respective digital certificates when provisioning the mobile devices, to enable the mobile devices to authenticate provisioning messages from the primary and secondary provisioning servers (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Claim 34 is rejected as applied above in rejecting claim 32. Furthermore, Penders discloses:

A machine-readable program storage medium as recited in claim 32, wherein the process further comprises specifying one or more parameters which the secondary provisioning server is authorized to provision in the mobile devices (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable

Art Unit: 2131

functionality that the secondary provisioning server is allowed to perform on the mobile device.

Claim 35 is rejected as applied above in rejecting claim 32. Furthermore, Penders discloses:

A machine-readable program storage medium as recited in claim 32, wherein the process further comprises provisioning the mobile devices with information indicating authorization of a plurality of secondary provisioning servers to provision the mobile devices (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Claim 36 is rejected as applied above in rejecting claim 35. Furthermore, Penders discloses:

A machine-readable program storage medium as recited in claim 35, wherein the process further comprises specifying one or more parameters which each of the secondary provisioning servers is authorized to provision in the mobile devices (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Art Unit: 2131

Claim 37 is rejected as applied above in rejecting claim 36. Furthermore, Penders discloses:

A machine-readable program storage medium as recited in claim 36, wherein said specifying one or more parameters comprises assigning each of the secondary provisioning servers provisioning authorization of a different scope (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device, wherein the functions can be different between different service providers (column 5 lines 44-61).

Claim 38 is rejected as applied above in rejecting claim 32. Furthermore, Penders discloses:

A machine-readable program storage medium as recited in claim 32, wherein the primary provisioning server has unrestricted authorization to provision the mobile devices, and authorization of the secondary provisioning server to provision the mobile devices is regulated by the primary provisioning server (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device, wherein the functions can be different between different service providers (column 5 lines 44-61).

Regarding claim 40, Penders discloses:

A method of operating a mobile device on a wireless network, the method comprising:

receiving a provisioning message from a first trusted provisioning domain (TPD), the provisioning message specifying a second TPD and indicating a parameter which the second TPD is authorized to provision in the mobile device (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device;

storing information identifying the second TPD and the parameter in response to the provisioning message (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device; and

provisioning the parameter in the mobile device in response to a provisioning message from the second TPD (column 7 lines 1-13).

Claim 41 is rejected as applied above in rejecting claim 40. Furthermore, Penders discloses:

A method as recited in claim 40, wherein the first TPD is within a trusted environment, and the second TPD is outside the trusted environment (Figure 1, column 5 lines 1-14), wherein the certificate authority is connected via a telecommunications network to the terminal and the Service Provider.

Art Unit: 2131

Claim 42 is rejected as applied above in rejecting claim 41. Furthermore, Penders discloses:

A method as recited in claim 41, further comprising:

receiving a digital certificate of the second TPD from the first TPD (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device; and

using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Claim 43 is rejected as applied above in rejecting claim 40. Furthermore, Penders discloses:

A method as recited in claim 40, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, the method further comprising storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device, wherein the functions can be different between different service providers (column 5 lines 44-61).

Regarding claim 44, Penders discloses:

A method of operating a mobile device on a wireless network, the method comprising:

receiving a provisioning message from a remote source, the provisioning message specifying a parameter (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain functions;

determining whether the remote source is a primary trusted provisioning domain (TPD) (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain functions;

if the remote source is the primary TPD, provisioning the parameter in the mobile device in response to the provisioning message (column 6 lines 1-25, column 6 line 63 – column 7 line 12);

if the remote source is not the primary TPD, determining whether the remote source is a secondary TPD authorized to provision the parameter, based on a provisioning authorization previously received by the mobile device from the primary TPD (column 6 lines 1-25, column 6 line 63 – column 7 line 12); and

if the remote source is a secondary TPD authorized to provision the parameter, provisioning the parameter in the mobile device in response to the provisioning message (column 7 lines 1-13).



Claim 45 is rejected as applied above in rejecting claim 44. Furthermore, Penders discloses:

A method as recited in claim 44, wherein the primary TPD operates within a trusted environment, and the secondary TPD operates outside the trusted environment (Figure 1, column 5 lines 1-14), wherein the certificate authority is connected via a telecommunications network to the terminal and the Service Provider.

Claim 46 is rejected as applied above in rejecting claim 44. Furthermore, Penders discloses:

A method as recited in claim 44, further comprising:

receiving a digital certificate of the secondary TPD from the primary TPD (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain functions; and

using the digital certificate in the mobile device to authenticate the provisioning message (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Claim 47 is rejected as applied above in rejecting claim 44. Furthermore, Penders discloses:

A method as recited in claim 44, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, the method further comprising storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message (column 6 lines 17-25).

Regarding claim 48, Penders discloses:

A mobile device configured to operate on a wireless network, the mobile device comprising:

a processor (column 3 lines 12-20);

a data communication device coupled to the processor to communicate data with one or more remote systems via the wireless network (column 5 lines 1-13); and

a memory coupled to the processor and storing instructions for execution by the processor to configure the mobile device to execute a process comprising:

receiving a provisioning message from a first trusted provisioning domain (TPD) via the wireless network, the provisioning message specifying a second TPD and indicating a parameter which the second TPD is authorized to provision in the mobile device (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain functions;

storing information identifying the second TPD and the parameter in response to the provisioning message (column 6 lines 17-25); and

provisioning the parameter in the mobile device in response to a provisioning message from the second TPD (column 7 lines 1-13).

Claim 49 is rejected as applied above in rejecting claim 48. Furthermore, Penders discloses:

A mobile device as recited in claim 48, wherein the first TPD is within a trusted environment, and the second TPD is outside the trusted environment (Figure 1, column 5 lines 1-14), wherein the certificate authority is connected via a telecommunications network to the terminal and the Service Provider.

Claim 50 is rejected as applied above in rejecting claim 49. Furthermore, Penders discloses:

A mobile device as recited in claim 49, wherein the process further comprises:  
receiving a digital certificate of the second TPD from the first TPD (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain functions; and

using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Art Unit: 2131

Claim 51 is rejected as applied above in rejecting claim 48. Furthermore, Penders discloses:

A mobile device as recited in claim 48, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, and wherein the process further comprises storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message (column 6 lines 17-25).

Regarding claim 52, Penders discloses:

A mobile device configured to operate on a wireless network, the mobile device comprising:

- a processor (column 3 lines 12-20);

- a data communication device coupled to the processor to communicate data with one or more remote systems via the wireless network (column 5 lines 1-13); and

- a memory coupled to the processor and storing instructions for execution by the processor to configure the mobile device to execute a process comprising

- receiving a provisioning message from a remote source, the provisioning message specifying a parameter (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain functions;

determining whether the remote source is a primary trusted provisioning domain (TPD) (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain functions;

if the remote source is the primary TPD, provisioning the parameter in the mobile device in response to the provisioning message (column 6 lines 1-25, column 6 line 63 – column 7 line 12);

if the remote source is not the primary TPD, determining whether the remote source is a secondary TPD authorized to provision the parameter, based on a provisioning authorization previously received by the mobile device from the primary TPD (column 6 lines 1-25, column 6 line 63 – column 7 line 12); and

if the remote source is a secondary TPD authorized to provision the parameter, provisioning the parameter in the mobile device in response to the provisioning message (column 7 lines 1-13).

Claim 53 is rejected as applied above in rejecting claim 52. Furthermore, Penders discloses:

A mobile device as recited in claim 52, wherein the primary TPD operates within a trusted environment, and the secondary TPD operates outside the trusted environment (Figure 1, column 5 lines 1-14), wherein the certificate authority is connected via a telecommunications network to the terminal and the Service Provider.

Claim 54 is rejected as applied above in rejecting claim 52. Furthermore, Penders discloses:

A mobile device as recited in claim 52, wherein the process further comprises:  
receiving a digital certificate of the secondary TPD from the primary TPD (Figure 1, column 6 line 64 – column 7 line 13), wherein the Certificate Authority (CA), transmits a certificate specifying that the Service Provider (secondary provisioning server) is allowed to perform certain functions; and

using the digital certificate in the mobile device to authenticate the provisioning message (column 6 lines 1-25, column 6 line 63 – column 7 line 12), wherein the certificate contains the allowable functionality that the secondary provisioning server is allowed to perform on the mobile device.

Claim 55 is rejected as applied above in rejecting claim 52. Furthermore, Penders discloses:

A mobile device as recited in claim 52, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, and wherein the process further comprises storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message (column 6 lines 17-25).

### ***Conclusion***


Art Unit: 2131

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA  
11/24/2006

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100